Mozes Magyar
mmagyar
20247055

1.
    a) by default Tor uses three hops so knowing the first means knowing the second and knowing the third(last) means knowing the second. So any traffic that has a common node can be thought to be the same line of communication and imply who is doing what.
    b) An obvious reason to want to not be an exit-relay is that if your governing body is strict then any data and connections coming from your computer could be treated as if you were the originator: any malicious or illegal traffic would be unencrypted on one side and be incriminating on you, which is undesirable.
    c) Data! Data are an invaluable resource these days for analysis and collection. Knowing the data flowing through an exit node means you get the unencrypted data and can analyze the types of data that people want anonymous connections for.
    d)
2.
3. d) Fingerprints are important because they offer a quick way to verify the owner of a key, if you fail to check a fingerprint you may be susceptible to an attack where an impostor gives you a fake fingerprint and send data directly to an eavesdropper. fingerprints should be checked by talking with the owner of the key directly, such as in person or over the phone.
4.
    a) 0C0C000618001341000000000000000 is an IV that gives my username instead of aaaaaaaa, more specifically it gives “mmagyar ” including a trailing space for padding. The reason it works is because CBC decrypts the ciphertext then XORs it with the IV (for the first block) so all I had to do was find what, when XORed with aaaaaaaa, gives my username and use that instead of a blank IV.
    b) Authenticity is the principle being violated. I would fix it by padding the plaintext with something at the beginning since the IV only influences the first block when deciphered.